UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/814,337 | 03/21/2001 | William J. Bolosky | MS1-735US | 3684 |

22801 7590 09/13/2004

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

| EXAMINER | |
|---|---|
| GYORFI, THOMAS A | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2135 | |

DATE MAILED: 09/13/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) |
|---|---|---|
| | 09/814,337 | BOLOSKY ET AL. |
| | Examiner | Art Unit |
| | Tom Gyorfi | 2135 |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *9/22/03 & 2/13/04*.

4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☒ Other: *IDS (PTO-1449) dated 8/5/04*.

1. Claims 1-18 have been examined.

### *Double Patenting*

2. Claims 5-8 are objected to under 37 CFR 1.75 as being a substantial duplicate of claims 1-4. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

### *Claim Rejections - 35 USC § 102*

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-8 are rejected under 35 U.S.C. 102(e) as anticipated by or, in the alternative, under 35 U.S.C. 103(a) as obvious over Chan (U.S. Patent 6,748,538).

Regarding claims 1 and 5, Chan teaches a method for ensuring the integrity of data, the method comprising a means for creating a signed manifest including the step of digitally signing the batch of files (Chan, column 4, lines 7-

10). Note that Chan goes on to further disclose that a secondary manifest can be created in a similar fashion, and both the signature of the manifest as well as the individual hash signatures of the files contained within can be compared to the corresponding values of the original manifest to determine if any changes were made (Chan, column 4, lines 11-47). Thus, it can be construed that the second manifest is a collection of changes that are made to multiple files stored in the file system.

In the event that Applicant disagrees with that interpretation, it would have been obvious to one of ordinary skill in the art at the time of the invention to use the method disclosed by Chan on a collection of files that the user knows have been changed. Recall that one of the primary purposes for the invention disclosed by Chan is to safeguard one's data against malicious alteration, as by a computer virus (Chan, column 1, lines 43-52). Users, however, will require the ability to make authorized modifications to their data, including data protected by the method disclosed by Chen. One would need to create a new manifest in the event that any file referenced within is deliberately changed; therefore it is obvious that a user would deliberately choose to execute the method disclosed by Chan on a collection of changed files that the user has personally modified.

Regarding claims 2 and 6, note that Chan discloses that each file to be stored in a manifest has a hash value computed for it (Chan, column 4, lines 1-3). Further, the hash values are collected together to form a manifest prior to being digitally signed (Chan, column 4, lines 3-4).

Regarding claims 3 and 7, note that the manifest produced by the method disclosed by Chan (Chan, element 260 of Figure 3) qualifies as a data structure under the broadest definition of the term.

Regarding claims 4 and 8, note that the method disclosed by Chan is embodied by computer-executable instructions contained in a computer-readable medium (Chan, column 2, lines 46-57).

### *Claim Rejections - 35 USC § 103*

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 9, 12, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan (U.S. Patent 6,748,538).

Regarding claim 9, Chan teaches a method to verify the integrity of a plurality of software components. This method includes the steps of computing a hash value of each file to be protected (Chan, column 4, lines 1-3), collecting the hash values into a group (Chan, column 4, lines 3-4), computing the hash value of the group (Chan, column 4, lines 4-7), and digitally signing the hash value of the group of hash values (Chan, column 4, lines 7-10). Chan is silent, however, on the nature of the software components to be protected; specifically, there is no mention of using encrypted files as part of the method to create a signed

manifest. It would have been obvious to one of ordinary skill in the art at the time of the invention disclosed by Applicant that one could use encrypted files as the software components to be protected using the method disclosed by Chan. Encryption is a technique that is well known in the art as a method of protecting data. Since the method disclosed by Chan is also intended to protect a user's data by ensuring that the data in question has not been altered, it stands to reason that encrypting the files prior to constructing a manifest adds an additional layer of security to the process.

Regarding claim 12, note that the manifest produced by the method disclosed by Chan (Chan, element 260 of Figure 3) qualifies as a data structure under the broadest definition of the term.

Regarding claim 13, note that the method disclosed by Chan is embodied by computer-executable instructions contained in a computer-readable medium (Chan, column 2, lines 46-57).

7. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan as applied to claim 9 above, and further in view of Amberden (U.S. Patent Application Publication 2002/0103818) and Moulton et al. (U.S. Patent 6,704,730).

Regarding claims 9 and 10, Chan does not teach a metadata stream comprising a header and per user information. However, Amberden discloses a repository database for file data that includes a metadata stream. Amberden is deemed to be analogous prior art because both it and the instant application are

from the same field of endeavor, namely the file format for data storage. The metadata stream contains a Stream Identification Number (Amberden, para. 148, "Stream entries and data records...") which can be understood to fulfill a similar function as the header disclosed by Applicant. Further, the metadata stream contains information such as information changes, storage locations, item types, and author IDs, among other things (Amberden, para. 149). This can be understood to fulfill a similar function to the per user data disclosed by Applicant. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention by Applicant to incorporate the functionality of a metadata stream such as the one disclosed by Amberden into a file system on which the method disclosed by Chan operates. By tracking metadata via a stream, one can more easily integrate information from disparate, diverse, isolated sources into a unified whole (Amberden, para. 304). It would be optimal for this information to be taken into account as part of the process disclosed by Chan.

Further regarding claims 9 and 10, neither Chan nor Amberden teaches an indexing structure, notably a tree containing a root node and branches as per claim 10, containing hashes of files. However, Moulton discloses a hash file system for use in a distributed computing environement (Moulton, column 7, lines 21-24) that comprises a tree with accessible nodes containing hash values of files (Moulton, column 11, lines 43-51; and Figure 9). By definition, a tree (as understood in the context of the art) possesses a root node and can possess one or more branch nodes, as illustrated in Figure 9. In addition, the nodes contain hashes of individual pieces of any given file (Moulton, column 10, lines 19-34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention disclosed by Applicant to include the index tree disclosed by Moulton as part of the metadata stream used in the combination of Chan and Amberden. Since the hashes constitute data about the file but are not actually part of the payload of the file, they qualify as being metadata under the commonly accepted definition for the term in the art. Further, by keeping hashes of pieces from the same file, an integrity scanning process (Chan, column 4, lines 11-47) can more easily pinpoint the specific part of a file that has been modified, whether by an authorized user or a malicious virus.

Further regarding claims 9 and 10, note that Chan teaches that software components undergo a one-way hash function to produce a corresponding digest (Chan, column 4, lines 1-3). While it is not explicitly stated what constitutes a software component, it would have been obvious to one of ordinary skill in the art at the time of the invention disclosed by Applicant that the metadata stream produced in the combination of Chan, Amberden, and Moulton would be included, and consequently the header, per user information and the root node would be hashed. It would be necessary to keep track of changes to the metadata as part of an integrity-scanning scheme, as even small changes could have significant consequences. For example, if the permissions of a confidential file were altered to make it publicly accessible, and the alterations were done without the authorized user's knowledge, an integrity scanner method such as the one disclosed by the combination of Chan, Amberden, and Moulton (based on Chan, column 4, lines 11-47) would detect it and the user could be notified.

8. Claims 14, 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chan, and further in view of Anderson et al. ("Serverless Network File Systems", Feb. 1996).

Regarding claim 14, again note that the invention disclosed by Chan comprises a computer-readable medium containing executable instructions to compute the hash of each file to be listed in a manifest (Chan, column 4, lines 1-3), collect the hash files into a group (Chan, column 4, lines 3-4), and digitally sign the group of hash values (Chan, column 4, lines 4-10). However Chan is silent as to the underlying nature of the file system upon which his invention can be implemented.

Applicant has submitted the article by Anderson et al. as prior art. Anderson teaches an experimental file system designated xFS, which is both serverless and distributed by design (Anderson, Chapter 1, "In contrast to central server designs..."). It can be reasonably inferred that among the features of xFS is the ability to modify individual files (Anderson, Chapter 3.2.3, "Cache Consistency"). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention disclosed by Applicant to implement the method disclosed by Chan on top of a serverless distributed file system such as the one disclosed by Anderson. In doing so, one gains additional scalability and improved performance (Anderson, Chapter 1, "A serverless network file system...") above that which one would obtain using the single computer platform as in the preferred embodiment of the invention disclosed by Chan.

Regarding claim 17, again note that the invention disclosed by Chan creates a manifest, the manifest being a data structure in the broadest definition of the term, comprising a digital signature covering at least part of the hashes representing the files referenced within (Chan, column 3, lines 48-62). With respect to the hashes representing modifications of files, see the rationale for rejection of claims 1 and 5. In addition, the claim specifically stipulates that the files are stored on a distributed file system; Chan is silent regarding the underlying file system upon which his disclosure is implemented. However, recall that Anderson teaches the use of a distributed file system possessing improvements in performance over the prior art (Anderson, Chapter 1, "A serverless network file system..."). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention disclosed by Applicant to implement the manifest data structure disclosed by Chan on top of a distributed file system such as the one disclosed by Anderson. In doing so, one gains the aforementioned performance enhancements above that which one would obtain using the single computer platform as in the preferred embodiment of the invention disclosed by Chan.

Regarding claim 18, again note that the manifest created by the invention disclosed by Chan contains hashes of data in each file (Chan, column 3, lines 48-60).

9. Claims 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Chan and Anderson as applied to claim 14

above, and further in view of Amberden (U.S. Patent Application Publication 2002/0103818) and Moulton et al. (U.S. Patent 6,704,730).

Regarding claims 15 and 16, neither Chan nor Anderson teaches a metadata stream comprising a header and per user information. However, Amberden discloses a repository database for file data that includes a metadata stream. Amberden is deemed to be analogous prior art because both it and the instant application are from the same field of endeavor, namely the file format for data storage. The metadata stream contains a Stream Identification Number (Amberden, para. 148, "Stream entries and data records...") which can be understood to fulfill a similar function as the header disclosed by Applicant. Further, the metadata stream contains information such as information changes, storage locations, item types, and author IDs, among other things (Amberden, para. 149). This can be understood to fulfill a similar function to the per user data disclosed by Applicant. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention by Applicant to incorporate the functionality of a metadata stream such as the one disclosed by Amberden into a file system on which the method disclosed by Chan operates. By tracking metadata via a stream, one can more easily integrate information from disparate, diverse, isolated sources into a unified whole (Amberden, para. 304). It would be optimal for this information to be taken into account as part of the process disclosed by Chan.

Further regarding claims 15 and 16, neither Chan, Anderson, nor Amberden teaches an indexing structure, notably a tree containing a root node

and branches as per claim 16, containing hashes of files. However, Moulton discloses a hash file system for use in a distributed computing environement (Moulton, column 7, lines 21-24) that comprises a tree with accessible nodes containing hash values of files (Moulton, column 11, lines 43-51; and Figure 9). By definition, a tree (as understood in the context of the art) possesses a root node and can possess one or more branch nodes, as illustrated in Figure 9. In addition, the nodes contain hashes of individual pieces of any given file (Moulton, column 10, lines 19-34). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention disclosed by Applicant to include the index tree disclosed by Moulton as part of the metadata stream used in the combination of Chan, Anderson, and Amberden. Since the hashes constitute data about the file but are not actually part of the payload of the file, they qualify as being metadata under the commonly accepted definition for the term in the art. Further, by keeping hashes of pieces from the same file, an integrity scanning process (Chan, column 4, lines 11-47) can more easily pinpoint the specific part of a file that has been modified, whether by an authorized user or a malicious virus.

Further regarding claims 15 and 16, note that Chan teaches that software components undergo a one-way hash function to produce a corresponding digest (Chan, column 4, lines 1-3). While it is not explicitly stated what constitutes a software component, it would have been obvious to one of ordinary skill in the art at the time of the invention disclosed by Applicant that the metadata stream produced in the combination of Chan, Anderson, Amberden, and Moulton would

be included, and consequently the header, per user information and the root node would be hashed. It would be necessary to keep track of changes to the metadata as part of an integrity-scanning scheme, as even small changes could have significant consequences. For example, if the permissions of a confidential file were altered to make it publicly accessible, and the alterations were done without the authorized user's knowledge, an integrity scanner method such as the one disclosed by the combination of Chan, Anderson, Amberden, and Moulton (based on Chan, column 4, lines 11-47) would detect it and the user could be notified.

***Conclusion***

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- Carbajal, et al. (U.S. Patent 6,725,373) "Method and Apparatus for Verifying the Integrity of Digital Objects Using Signed Manifests"
- Carbajal et al. (U.S. Patent 6,560,706) "System for Ensuring Boot Image Integrity and Authenticity"
- Schmidt et al. (U.S. Patent 6,535,894) "Apparatus and Method for Incremental Updating of Archive Files"
- Cohen et al. (U.S. Patent 6,522,423) "Method and Apparatus in a Data Processing System for Generating Metadata Streams with Per Page Data"
- Cohen et al. (U.S. Patent 6,510,426) "Method and Apparatus for Compacting a Metadatas Stream in a Data Processing System"

- Drews (U.S. Patent 6,463,535) "System and Method for Verifying the Integrity and Authorization of Software Before Execution in a Local Platform"
- Cooper, et al. (U.S. Patent 6,295,538) "Method and Apparatus for Creating Metadata Streams with Embedded Device Information"

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tom Gyorfi whose telephone number is (571) 272-3849. The examiner can normally be reached on 8:00am - 4:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

TAG
08/31/04

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100